



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/620,772	07/21/2000	Raynold M. Kahn	PD-200045	3987

20991 7590 03/01/2004

HUGHES ELECTRONICS CORPORATION
PATENT DOCKET ADMINISTRATION RE/R11/A109
P O BOX 956
EL SEGUNDO, CA 90245-0956

EXAMINER

TRAN, ELLEN C

ART UNIT PAPER NUMBER

2134

DATE MAILED: 03/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/620,772

Applicant(s)

KAHN ET AL.

Examiner

Ellen C Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 July 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-42 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-42 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 3-7.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: original application filed 21 July 2000.
2. Claims 1-42 are currently pending in this application. Claims 1, 17, and 28 are independent claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

4. **Claims 1-15 and 17-41** are rejected under 35 U.S.C. 102(e) as being anticipated by Kocher et al. U.S. Patent No. 6,289,455 (hereinafter '455).

As to independent claim 1, "A method of storing program material for subsequent replay, comprising the steps of" is taught in '455 col. 5, lines 55-65 "The present invention can improve the security of systems used to distribute and protect digital content";

"(a) accepting encrypted access control information and the program material encrypted according to a first encryption key, the access control information including a first encryption key and control data; (b) decrypting the received access control information to produce the first encryption key; (d) re-encrypting the program material according to a second encryption key; (e) encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and (f) providing the re-

encrypted program material and the fourth encryption key for storage” is shown in ‘455 col. 16, line 47 through col. 17, line 10 “Fig. 9 diagrams the operation of an exemplary Crypto-Firewall that implements prepaid rights ...(i.e. (a) same as step 900, (b) same as step 930, (d) and (e) same as step 950, (f) same as step 910)”;

“(c) decrypting the program material using the first encryption key” is shown in ‘455 col. 11, lines 63-65 “At step 580, the ICP transmits the CDK to the playback device, which at step 590, uses the CDK to decrypt the content” (i.e. (c) same as step 590).

As to dependent claim 2, **“wherein the encrypted access control information further comprises temporally-variant control data, and the method further comprises the steps of. decrypting the received access control information to produce the temporally-variant control data; and modifying the temporally variant control data to generate temporally-invariant control data”** is taught in ‘455 col. 17, lines 1-4 “rights keys-are used to derive content decryption keys, so the results are not stored. Transformation protected with the CHIP_KEY are used to add new rights keys”.

As to dependent claim 3, **“wherein steps (b) and (e) are performed in a conditional access module”** is shown in ‘455 col. 21, lines 64-66 “In one preferred embodiment, the entire CRU is implemented in a single smartcard. Alternatively, the CRU can be a PCMCIA card ...”.

As to dependent claim 4, **“wherein the conditional access module is implemented on a smartcard”** is taught in ‘455 col. 21, lines 64-65 “In one preferred embodiment, the entire CRU is implemented in a single smartcard”;

“communicatively coupleable to a tuner and a media storage device” is taught in ‘455 col. 9, lines 10-15 “A variety of distribution methods may be employed, including without

Art Unit: 2134

limitation distribution of physical media (such as optical discs), radio or satellite transmission, wired networks (such as telephone, ADSL, cable television, etc.), and distribution over computer networks (such as publication on a web site, multicast, ect.)” (note: to receive a radio transmission a tuner is used).

As to dependent claim 5, “wherein the access control information further comprises metadata describing at least one right for the program related material” is disclosed in ‘455 col. 16, lines 47-49 “that implements prepaid rights but can be easily extended to support post-paid rights”.

As to dependent claim 6, “further comprising the step of- generating the second encryption key at least in part from the metadata” is disclosed in ‘455 col. 16, lines 47-49 “that implements prepaid rights but can be easily extended to support post-paid rights”.

As to dependent claim 7, “wherein steps (b)-(f) are performed in response to a pre-buy message” is shown in ‘455 col. 10 lines 50-55 “When a user purchases (or otherwise obtains) permission to use some content, the playback device receives an appropriate rights enablement message (REM)”.

As to dependent claim 8, this claim incorporates substantially similar subject matter as in claims 5 and 6 and is rejected along the same rationale.

As to dependent claim 9, “wherein the replay right data is further generated from pre-buy data” is shown in ‘455 col. 10 lines 50-55 “When a user purchases (or otherwise obtains) permission to use some content, the playback device receives an appropriate rights enablement message (REM)”.

As to dependent claim 10, this claim incorporates substantially similar subject matter as in claims 2 and is rejected along the same rationale.

As to dependent claim 11, “wherein the step of decrypting the fourth encryption key using the third encryption key to produce the second encryption key” is taught in ’455 col. 17, lines 1-4 “rights keys-are used to derive content decryption keys”;

“is performed in response to a subscriber request to access the program material” is shown in ’455 col. 10 lines 50-55 “When a user purchases (or otherwise obtains) permission to use some content, the playback device receives an appropriate rights enablement message (REM)”.

As to dependent claim 12, “wherein the access control information further comprises metadata describing at least one right for the program material” is disclosed in ’455 col. 16, lines 47-49 “that implements prepaid rights but can be easily extended to support post-paid rights”;

“the subscriber request to access the program material comprises buy data” is shown in ’455 col. 10 lines 50-55 “When a user purchases (or otherwise obtains) permission to use some content, the playback device receives an appropriate rights enablement message (REM)”.

“ and the method further comprises the steps of generating replay right data from the metadata accepting the buy data; comparing the buy data with the replay right data and decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data” is taught in ’455 col. 17, lines 1-4 “rights keys-are used to derive content decryption

keys, so the results are not stored. Transformation protected with the CHIP_KEY are used to add new rights keys”.

As to dependent claim 13, “wherein steps (b)-(f) are performed in response to a pre-buy message” is shown in ‘455 col. 10 lines 50-55 “When a user purchases (or otherwise obtains) permission to use some content, the playback device receives an appropriate rights enablement message (REM)”.

“and wherein: the second encryption key and the third encryption key are stored in a smartcard” is shown in ‘455 col. 21, lines 64-66 “In one preferred embodiment, the entire CRU is implemented in a single smartcard. Alternatively, the CRU can be a PCMCIA card ...”

“and the replay right data is generated from the metadata and the pre-buy message in the smartcard and the steps of accepting the buy data, comparing the buy data with the replay right data, and decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data are performed in the smartcard” is disclosed in ‘455 col. 17, lines 1-4 “rights keys-are used to derive content decryption keys, so the results are not stored. Transformation protected with the CHIP_KEY are used to add new rights keys”.

As to dependent claim 14, “wherein the re-encrypted program material and the fourth encryption key are stored on a media storage device” is taught in ‘455 col. 9, lines 10-15 “A variety of distribution methods may be employed, including without limitation distribution of physical media (such as optical discs), radio or satellite transmission, wired networks (such as

telephone, ADSL, cable television, etc.), and distribution over computer networks (such as publication on a web site, multicast, ect.)”.

As to dependent claim 15, “wherein the control data is temporally-variant” is taught in ’455 col. 17, lines 1-4 “rights keys-are used to derive content decryption keys, so the results are not stored. Transformation protected with the CHIP_KEY are used to add new rights keys”.

As to dependent claim 17, “further comprising: a tuner, communicatively coupleable to the conditional access module” is taught in ’455 col. 9, lines 10-15 “A variety of distribution methods may be employed, including without limitation distribution of physical media (such as optical discs), radio or satellite transmission, wired networks (such as telephone, ADSL, cable television, etc.), and distribution over computer networks (such as publication on a web site, multicast, ect.)” (note: to receive a radio transmission a tuner is used).

“for receiving the encrypted access control information and the program material encrypted according to a first encryption key; a third decryption module, for decrypting the program material using the first encryption key produced by the conditional access module; a second encryption module, for re-encrypting the decrypted program material according to the second encryption key; and a fourth decryption module, for decrypting the re-encrypted program material according to the second encryption key” is taught in ’455 col. 17, lines 1-4 “rights keys-are used to derive content decryption keys, so the results are not stored. Transformation protected with the CHIP_KEY are used to add new rights keys”.

As to dependent claim 18, this claim incorporates substantially similar subject matter as in claims 17 and is rejected along the same rationale.

As to dependent claim 19, this claim incorporates substantially similar subject matter as in claims 7 and is rejected along the same rationale.

As to dependent claim 20, this claim incorporates substantially similar subject matter as in claims 5 and is rejected along the same rationale.

As to dependent claim 21, this claim incorporates substantially similar subject matter as in claims 6 and 7, and is rejected along the same rationale.

As to dependent claim 22, “further comprising a buy module, communicatively coupled to the pre-buy module” is shown in ‘455 col. 10 lines 50-55 “When a user purchases (or otherwise obtains) permission to use some content, the playback device receives an appropriate rights enablement message (REM)”.

As to dependent claim 23, “, further comprising a billing module, for recording the buy data” is disclosed in ‘455 col. 9, lines 60-62 “A communication channel from CRU 225 to content provider 200 is also provided for auditing post-payment purchases”.

As to dependent claim 24, “wherein the second encryption key is stored in the conditional access module” is disclosed in ‘455 col. 16, lines 50-52 “the CryptoFirewall contains a device key (CHIP_KEY) as well as memory locations for storing prepaid rights keys”.

As to dependent claim 25 and 26, these claims incorporate substantially similar subject matter as in claims 24 and are rejected along the same rationale.

As to dependent claim 27, this claim incorporates substantially similar subject matter as in claims 17 and is rejected along the same rationale.

As to independent claims 28, this claim is directed to an apparatus of the method of claim 1 and is similarly rejected along the same rationale.

As to dependent claim 29-41, these claims incorporate substantially similar subject matter as in cited in the claims above and are rejected along the same rationale.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 16 and 42** are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘455 as applied to the claims above in further view of Sims, III U.S. Patent No. 6,550,011 B1 (hereinafter ‘011).

As to dependent claim 16, the following is not taught in exact terminology in ‘455: “wherein the temporally-variant control data associates an expiration time with the program material” however ‘011 teaches “for storing content use information. Such information may include a generation counter, generation limit, copyright status indication, expiration information, watermark verification data, region coding, byte count limits, time limits, expiration based on the end of the content, and the like” in col. 11, lines 33-41.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in ‘455 to include a method replay time. One of ordinary skill in the art would have been motivated to perform such a modification because a need exist for a more versatile method to allow distribution and protect

digital content see '011 (col. 3, lines 55 et seq.) "Likewise, a need exists in the art for a more robust set of rules establishing authorized utilization of content".

As to dependent claim 42, this claim incorporates substantially similar subject matter as in claims 16 and is rejected along the same rationale.


Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5484.

Ellen Tran
Patent Examiner
Technology Center 2134
17 February 2004


NORMAN M. WRIGHT
PRIMARY EXAMINER